REMARKS

Claims 1-39 are pending in the present application. Claims 1, 5, 8, 16, 19, 21, 22, 26, 29, 37, and 38 were amended. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. 35 U.S.C. § 112, First Paragraph

The examiner has objected to claim 1 under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Additionally, the examiner rejected the claims under the same reasons. This rejection is respectfully traversed.

In rejecting claim 1, the examiner stated:

> Claim1 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.
>
> The limitation of "receiving the content from the source, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content" contradicts the limitation of "selectively preventing receipt of the content from the source." Furthermore the specification does not support this contradiction.
>
> Evidence that claim 1 fail(s) to correspond in scope with that which applicant(s) regard as the invention can be found in page no. 15, lines 2-19 of the specification. On that page, the application has stated "*If the user at client 400 suspects monitoring is occurring when retrieving a Web page from server 402, a request may be sent to validation server 410 to determine whether such a situation is occurring. ...In response to receiving the request from client 400, validation engine 412 sends requests to Web server 402 for Web pages using the set of URLs. URLs in the retrieved content are compared...*". This paragraph in the applicant's specification indicates that the invention is different from what is defined in the Claim(s) limitation whereby the second limitation of Claim 1 discloses "receiving the content from the source" and "selectively preventing receipt of the content from the source. The former and latter limitation of Claim 1 furthermore contradict themselves because on one end the client apparently receives the content from the source before any validation of the content is performed, contrary to the applicant's quoted specification. Afterwards, following the negative response indicating monitoring of the user requests, the

receipt of the content from the source is selectively prevented. If the content from the source is already received, then how can receipt of the content from the source be prevented? These two limitations clearly contradict themselves and the attorney is kindly encouraged to make the necessary corrections.

For purposes of applying art the second limitation of Claim 1 and all other claims containing the limitation of "receiving the content from the source wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content" is considered.

Office Action dated June 4, 2004, pages 3-4.

In response to the examiner's comments, claim 1 has been amended as follows:

1. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:

requesting the content from a source using a set of identifiers;

receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content;

sending identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source; and

responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source.

As can be seen, claim 1 has been amended to recite that the preventing step selectively prevents receipt of additional content from the source, rather than the content itself. As a result, the feature in this step no longer conflicts with the feature in the requesting step of claim 1.

Therefore, the objection of to claim 1 under 35 U.S.C. § 112, first paragraph has been overcome.

II. 35 U.S.C. § 103, Obviousness

The examiner has rejected claims 1-38 under 35 U.S.C. § 103 as being unpatentable over Bryant, United States Patent No. 6286046 B1 ("*Bryant*") in view of www.junkbusters.com ("*Junkbusters*"). This rejection is respectfully traversed.

Claim 1

In rejecting the claims, the examiner stated the following:

With regards to Claim 1, Bryant meets the limitations of "requesting the content from a source" on column 3, lines 34-35; and "sending a set of identifiers used to reach the content to a validation service wherein the set of identifiers includes each identifier used to request the content" on column 3, lines 62-66, column 4, lines 50-64; and "each returned identifier representing the location of the content" on column 7, lines 66-67 and column 8, lines 1-19; The limitation of the indication of the monitoring of user requests to content and selectively preventing receipt of content is not met explicitly by Bryant. However, this limitation is met by www.junkbusters.com on page 2 and 3, paragraph 2. This reference discloses Internet Junkbusters 2.0.2 works as a proxy that checks every HTTP request against a list of URL's before delivering the content. Furthermore, it stops almost all cookies by deleting them, as long as the cookies are approved for deletion. Hence, it provides the capability of detecting monitoring of access to content (by detecting cookies) and selectively preventing receipt of content.
Bryant possesses a web browser, a web server and a monitor that represents the validation service. The monitor acts like the validation service because it logically sits in between the web browser at the client's side and one or more servers and acts as a proxy by redirecting requests on behalf of the client to the server and receiving and performing verification of the server's response. The monitor does not only record sessions (as assumed by the attorney) but performs simulation of requests and verification processes on the response received from the server, to see if it is a correct response (Bryant, column 4, lines 50-67, column 5, lines 1-25). A possible response could be a situation whereby an accessed website generates spyware data such as a cookie that can track/monitor the user's web activity.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of www.junkbusters.com to that of Bryant because utilizing the monitor as a proxy to prevent the download of spyware or adware to the client's computer would prevent the client's computer from falling prey to network clogging/slowing software from being downloaded without the user's permission. This spyware prevention systems/software i.e. detection/prevention of monitoring is already well known in the art.

Office Action dated June 4, 2004, pages 5-6.

A. The examiner bears the burden of establishing a *prima facie* case of obviousness.

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992).

In this particular case, the examiner has failed to establish a prima facie case of obviousness because the features believed to be taught by *Bryant* are not actually present in this reference.

B. All claim limitations must be considered, especially when missing from prior art.

In comparing the presently claimed invention with *Bryant* and *Junkbusters*, the features of the presently claimed invention may not be ignored in an obviousness determination.

The present invention in amended claim 1 recites:

> 1. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:
>
> requesting the content from a source using a set of identifiers;
>
> receiving the content from the source to form received content, wherein at least one returned identifier is returned from the source in which the at least one returned identifier represents a location of the content;
>
> sending identifiers to a validation service, wherein the identifiers includes the set of identifiers used to request the received content and each returned identifier representing the location of the content at the source; and
>
> responsive to receiving a response from the validation service indicating the monitoring of user requests to access to the received content is occurring, selectively preventing receipt of additional content from the source.

All of the features in claim 1 have not been properly considered by the examiner in stating that this claim is obvious in view of *Bryant* and *Junkbusters*. For example, the examiner has pointed to the following portions of *Bryant* for the step of sending a set of identifiers used to reach the content to a validation service:

> The primary function of the monitor **40** is to record a set of URLs (sometimes referred to as a "request list") that issue from the Web browser during an interactive sample session between the user of the client machine and the server application.

Bryant, column 3, lines 62-66. This portion of *Bryant* teaches using a monitor to record URLs issued by a browser. This portion of *Bryant*, however, provides no teaching, suggestion, or incentive for sending a set of identifiers used to reach content to a validation service. Further, the recording of URLs by monitor **40** in this particular cited portion is not the same as validating those URLs in claim 1. Nowhere is a validation service mentioned in *Bryant* in this cited section for the sending step of claim 1. Also, monitor **40** in this portion of *Bryant* does not provide an indication that monitoring is occurring as recited in the receiving step of claim 1. Such an indication is returned from the validation service in claim 1 if monitoring of access to content occurs. Consequently, this portion of *Bryant* does not teach or suggest the sending step in claim 1.

The examiner also points to the following portion of *Bryant* for this particular feature:

> As illustrated in **FIG. 2**, according to the invention, when the monitor is in use, all requests that would normally be sent to the server **36** are sent to the monitor **40** instead. The monitor **40** then forwards the requests to the actual server and receives the responses from the server **36**. Responses from the server are then returned from the monitor **40** to the browser **32**. In effect, the monitor **40** acts as an HTTP request/response forwarder that masquerades as the actual server (as far as the browser is concerned) and the actual browser (as far as the server is concerned). To achieve the masquerade, the monitor **40** translates the HTTP requests received from the browser **32** before sending these requests to the server, and it translates the HTTP responses and HTML received from the server before these responses are delivered to the browser. These translation functions are described below.

Bryant, column 4, lines 50-65. This cited portion of *Bryant* teaches that when monitor **40** is in use, all requests normally sent to the server are sent to monitor **40** instead. These requests are then forwarded to the server and responses are received from the server by monitor **40**. These responses are returned to browser **32** from monitor **40**. As can be seen, this portion of *Bryant* does not teach sending a set of identifiers used to reach the content of validation service in the manner recited in claim 1. Instead, this portion of

Bryant teaches forwarding requests that are normally sent by the browser to the server to monitor instead. As a result, these identifiers are not the ones used to request the content that forms the received content. Also, the identifiers sent to the monitor do not include each returned identifier representing the location of the received content. This feature was present in claim 1 prior to the amendment of this claim.

Further, claim 1 has been amended to clarify that the identifiers sent to the validation service include the identifiers that are used to request the received content from the source and identifiers returned when the content is received in which the returned identifiers represent the location of the received content at the source. Amended claim 1 specifically includes requesting content, receiving the content, and then sending the identifiers used to request the received content to a validation service after the content has been received.

In contrast, this portion of *Bryant* teaches using the monitor as a request and response forwarder, which is totally different from the manner in which the sending step operates when this sending step is viewed with respect to the other steps in claim 1. In other words, *Bryant* receives all of the requests from the browser and then sends those requests to the source or server and receives the response. The browser does not receive the content and then send the identifiers to the monitor. Thus, *Bryant* operates in a totally different fashion from the present invention as recited in amended claim 1. Therefore, *Bryant* does not teach or suggest the features of the presently claimed invention.

C. Stating that it is obvious to try or make a modification or combination without a suggestion in the prior art is not *prima facie* obviousness.

The mere fact that a prior art reference can be readily modified does not make the modification obvious unless the prior art suggested the desirability of the modification. *In re Laskowski*, 871 F.2d 115, 10 U.S.P.Q.2d 1397 (Fed. Cir. 1989) and also see *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992) and *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1993). The examiner may not merely state that the modification would have been obvious to one of ordinary skill in the art without pointing out in the prior art a suggestion of the desirability of the proposed modification.

In addition to not teaching the features of the presently claimed invention as believed by the examiner, no teaching, suggestion, or incentive has been provided in *Bryant* or *Junkbusters* for the possible response claimed by the examiner. Further, no teaching, suggestion, or incentive is provided in either reference to modify the monitor of *Bryant* to become a validation service that provides a response to indicate whether monitoring of user requests to access the received content is occurring. This feature is not found in either of the cited references.

For example, the examiner also believes that the monitor in *Bryant* performs a validation service by citing to the following portions of *Bryant*:

> As illustrated in **FIG. 2**, according to the invention, when the monitor is in use, all requests that would normally be sent to the server **36** are sent to the monitor **40** instead. The monitor **40** then forwards the requests to the actual server and receives the responses from the server **36**. Responses from the server are then returned from the monitor **40** to the browser **32**. In effect, the monitor **40** acts as an HTTP request/response forwarder that masquerades as the actual server (as far as the browser is concerned) and the actual browser (as far as the server is concerned). To achieve the masquerade, the monitor **40** translates the HTTP requests received from the browser **32** before sending these requests to the server, and it translates the HTTP responses and HTML received from the server before these responses are delivered to the browser. These translation functions are described below.
>
> As browser requests are received by the monitor **40**, the monitor performs the monitoring function or some other function as selected by options specified when the monitor is started. As has been described, the monitor function writes the set of URLs (i.e., the URL trace) to the file **44**. In addition to the Web requests, the monitor may also record information **48** (in the request file **44** or in some other file) characterizing the response received from the server. This characterization can be as simple as a checksum of the page returned from the server, or a more elaborate characterization. Such characterization can then be later used to verify that the response received from the server is a correct response. Thus, for example, a verification might involve matching a checksum to fully parsing and analyzing the HTML response. Any particular verification technique may be used.
>
> As discussed above, each HTTP submitter routine **46** takes a list of URLs and associated data, connects to a Web server, submits the URLs, and fetches the responses. This operation thus simulates the interactive session without having to run the server application against an actual client machine. Such "submitter" routines are well known and within the state-of-the-art. They are available in the literature or via download on the Internet. In the present invention, any suitable HTTP submitter routine **46**

> may be used to perform the replay function provided the program can read the particular request file format created by the monitor **40**.

Bryant, column 4, line 50-column 5, line 25. *Bryant* teaches in the cited section to determine whether the response received from the server is a correct response. This type of verification has nothing to do with determining whether monitoring of user requests to access the received content is occurring. The examiner states that a possible response could be a situation whereby accessed Websites generate spyware data such as a cookie that can track/monitor the user's Web activity. Such a feature is not taught or suggested by *Bryant*. The mere fact that such a modification could be made does not mean such a modification would be made by one of ordinary skill in the art. The examiner has provided no teaching, suggestion, or incentive for one of ordinary skill in the art to modify the monitor of *Bryant* to perform a validation service that indicates whether monitoring of user requests to access the received content is occurring. Therefore, a combination of *Bryant* with *Junkbusters* would not lead to the presently claimed invention.

D. The proposed modification of the cited references would not be made when the cited references are considered as a whole.

"It is impermissible with the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art." *In re Hedges*, 228 U.S.P.Q. 685, 687 (Fed. Cir. 1986). In considering the cited references as a whole, one of ordinary skill in the art would consider the problems recognized by each of these references in determining whether to combine these two references in the manner proposed by the examiner. *Bryant* is concerned with the following:

> Because an e-business application running on a Web server may have to support a large number of interactions in a given time period, measuring and tuning the performance of the application is an important goal. Similarly, because reliability and functional correctness of the e-business application are paramount, functional and system testing of the application are also important elements of the development process. Also, if an individual user of the e-business application encounters poor

> response time, it may be important from a customer service viewpoint to be able to quantify and measure the exact nature of the user's performance difficulty in order to resolve the problem. Such measurements should concentrate on the delay of the server as it interacts with the user as opposed to measuring performance characteristics of the client machine (e.g., how long it takes the browser to render the servers response on the client machine).
>
> An important part of performance measurement and system testing of an e-business application is the problem of capturing a test workload. A test workload is a set of URL requests that take place between a client application and a e-business application during a simulated or "sample" interactive session involving the application. A test workload, theoretically, could be replayed to the server for performance measurement or functional testing purposes. The prior art, however, does not provide any adequate means or method of compiling such workload information. A possible solution is a manual "monitoring" technique, wherein one could just watch the URLs that the browser submits and copy these URLs down by hand in order to create a list of requests to the application (i.e., a "request list"). For most e-business applications, however, the URLs are complex and hard to read due to "URL encoding". Copying the requests down by hand is thus extremely error prone for all but the simplest of e-business applications.
>
> Thus, there remains a need to provide a technique to monitor and record information about specific requests to a server application, such as an e-business application, to thereby generate "workload" information that may then be used for later playback to benchmark the server application.

Bryant, column 1, line 31-column 2, line 3.

As can be seen, *Bryant* is directed towards problems associated with performance measurement and system testing of an e-business application. *Bryant* recognizes that from a customer service viewpoint, quantifying and measuring the nature of poor response times for e-business applications is important. Specifically, *Bryant* recognizes that a need is present to monitor and record information about specific requests to a server application and to generate workload information used for benchmarking the application at a later time.

In contrast, *Junkbusters* is directed towards eliminating unwanted items while surfing the web. *Junkbusters* recognizes that users of browsers may encounter unwanted items such as ads and cookies while browsing. Thus, Bryant and Junkbusters are both directed towards vastly different problems. One of ordinary skill in the art, in

considering these references as a whole, would not be motivated to combine these references or modify them in any manner proposed by the examiner.

In further considering these references as a whole, one of ordinary skill in the art would consider the solutions provided by the references. In this particular case, in providing a solution, *Bryant* teaches the following:

> The present invention provides a monitor tool that preferably sits between a Web browser and a server upon which a server application is running. The monitor tool is useful for recording a set of URLs (sometimes referred to as a "request list") that issue from the Web browser during a sample interactive session between the user of the client machine and the server application. The URL request list trace or session "workload" may then be used to benchmark the server application by supplying the information as an input to a set of HTTP submitter routines. Each HTTP submitter routine simulates a particular user of a client machine connected to the server application. Each routine then "replays" the interactive session recorded by the monitor so that the overall performance of the server application against "multiple" simulated users may be evaluated.
>
> The monitor tool is provisioned such that, from the browser's perspective, the tool appears to be the server itself; likewise, from the server's perspective, the tool appears to be the browser. Moreover, communications between the browser and the monitor are carried out in an unencrypted manner, although the monitor provides whatever secure connection (e.g., a secure sockets layer ("SSL") connection) that is expected or may be required with respect to the communications to and from the server. The monitor further includes a link substitution algorithm that prevents the browser from escaping from the connection to the monitor. In addition, the monitor tool may also be used to measure response times associated with the interactive session.

Bryant, column 2, line 6-32. *Bryant* teaches a solution in which a monitor tool is used to act like a browser to measure response times for an interactive session.

In contrast, *Junkbusters* teaches the following solution:

> The Internet Junkbuster Proxy™ gets rid of stuff you don't want while surfing the Web, such as banner ads and cookies. It's free software that everyone is welcome to download, install and distribute (according to the GPL). It uses very little disk space and is so fast that it's practically unnoticeable. If ads are blocked, it typically speeds up surfing.
>
> - The current release, Internet Junkbuster 2.0.2, works as a *proxy* that stands between your browser and the Internet, checking every HTTP request for each resource (including graphics) against a *blockfile* of URLs before sending it over

the Internet. (It can also be configured as a plain old non-caching, non-blocking proxy.)

- The Internet Junkbuster can be used with almost any web browser. It's very small, but it's not a plug-in.
- The code compiles on a very wide range of computing environments. A binary (.exe) for Windows 95/NT is included.
- The C source code and documentation are available for free download as a zip or tar file for you to use as long as you wish under the GNU General Public License (GPL). It comes with no warranty.
- If you are running a Mac operating system, ask your ISP or systems administrator at work to set if up on one of their servers or consider alternatives such as interMute, WebFree or Muffin.
- If you notice an ad or anything you don't want getting through, you simply add a pattern covering it to your blockfile. The Internet Junkbuster can also be used to block whole sites.
- The Internet Junkbuster stops almost all cookies, except from sites you tell it are allowed to set cookies. It also helps prevent the disclosure of other details that surfers often want kept private, such as information about the page clicked on, and their computer's software and hardware configuration. These features can be optionally disabled or altered.
- For more information see our comprehensive page of Frequently-Asked Questions the more technical manual, or the page of distribution information, which explains the versions and platforms available.
- The mission of Junkbusters is to free the world from junk communications. If you find that the Internet Junkbuster improves the quality of your life online, please tell others about it and help them install it. We also hop you'll examiner our free services that help you bust the other kinds of junk out of your life.

Junkbusters, page 2. As can be seen, this particular reference teaches a program that works as a proxy between the browser and the Internet. This proxy checks every request for each resource against a blockfile of URLs. If the URL is found, then that content is blocked from reaching the browser. Therefore, *Junkbusters* teaches a totally different solution from the one provided in *Bryant*. *Bryant* teaches a monitoring tool to measure response times, while *Junkbusters* teaches a proxy for blocking content.

Thus, these two references address different problems and solutions. *Bryant* is addressing performance issues associated with e-applications, while *Junkbusters* addresses problems associated with unwanted content, such as ads and cookies, that are received while surfing the web. Further, both references also provide entirely different solutions to these problems. For example, *Bryant* provides a monitor used to mimic or act as a browser for measuring response times. In contrast, *Junkbusters* provides a proxy that sits between the browser and the Internet to block unwanted content based on comparing the URL being sent over the Internet with a list of URLs.

Thus, one of ordinary skill in the art would not be motivated to combine these references and modify them in the manner suggested by the examiner when these references are considered as a whole.

E. The presently claimed invention may be reached only through an improper use of the disclosed invention as a template to piece together and modify the prior art.

Moreover, the examiner may not use the claimed invention as an "instruction manual" or "template" to piece together the teachings of the prior art so that the invention is rendered obvious. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Such reliance is an impermissible use of hindsight with the benefit of applicants' disclosure. *Id.*

Therefore, absent some teaching, suggestion, or incentive in the prior art, *Bryant* and *Junkbusters* cannot be properly combined to form the presently claimed invention. These two references are directed towards different problems and solutions. No teaching, suggestion, or incentive is present in either of these references to combine them in the manner proposed by the examiner. As a result, absent any teaching, suggestion, or incentive from these references or elsewhere in the prior art to make the proposed combination, the presently claimed invention can be reached only through an impermissible use of hindsight with the benefit of applicant's disclosure as a model for the needed changes.

Claim 8

With respect to **claim 8**, the examiner states the following.

> With respect to Claim 8, Bryant meets the limitations of "receiving a request from a requestor...wherein the request includes a set of identifiers used to access selected content" is met on column 3, lines 62-66; and "in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number identifiers represents a location of the content returned to the requestor in response to the first number of identifiers" on column 3, lines 59-66, column 7, lines 66-67, column 8, lines 1-19 and 31-41; and "sending a new request using an identifier from the first number of identifiers in the set of identifiers" is met on column 4, lines 15-24; and "receiving a first response from the source wherein the response includes a return identifier" on column 4, lines 53-56; and "comparing the set of identifiers to the return identifier and generating a second response ...by the source in response to an absence of a match between the identifier and any identifier in the set of identifiers" inherently on column 5, lines 3-14. Bryant however does not meet the limitation of indication of monitoring of access. This is however met by www.junkbusters.com on page 2 and 3, 2nd paragraph. The cookies detected represent the detection of monitoring of access because this is the inherent function of a cookie.
>
> It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of www.junkbusters.com to that of Bryant because utilizing the monitor as a proxy to prevent the download of spyware or adware to the client's computer would prevent the client's computer from falling prey to network clogging/slowing software from being downloaded without the user's permission. This spyware prevention systems/software i.e. detection/prevention of monitoring is already well known in the art.

Office Action dated June 4, 2004, pages 8-9.

Claim 8 reads as follows:

> 8. A method in a data processing system for detecting monitoring of access to content, the method comprising the data processing system implemented steps of:
>
> receiving a request from a requestor to determine whether a source of the content is monitoring access by the requestor, wherein the request includes a set of identifiers used to access selected content in which the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned by the source in which the second number of identifiers represents a

> location of the content returned to the requestor in response to the first number of identifiers;
>
> sending a new request to the source using an identifier from the first number of identifiers in the set of identifiers;
>
> receiving a first response from the source, wherein the response includes a return identifier;
>
> comparing the set of identifiers to the return identifier; and
>
> generating a second response indicating the monitoring of access by the requestor for content by the source in response to an absence of a match between the return identifier and any identifier in the set of identifiers.

Bryant does not teach all of the features that the examiner believes are present for claim 8. Specifically, the comparing and generating steps in claim 8 are not taught in *Bryant* as believed by the examiner.

The examiner points to the following portion of this cited reference for the comparing and generating step:

> In addition to the Web requests, the monitor may also record information 48 (in the request file 44 or in some other file) characterizing the response received from the server. This characterization can be as simple as a checksum of the page returned from the server, or a more elaborate characterization. Such characterization can then be later used to verify that the response received from the server is a correct response. Thus, for example, a verification might involve matching a checksum to fully parsing and analyzing the HTML response. Any particular verification technique may be used.

Bryant, column 5, lines 3-14. This portion of *Bryant* does not teach comparing the set of identifiers to a return identifier and generating a second response indicating the monitoring of access in response to an absence of a match. *Bryant* only discusses characterizing information received from the server in which the characterization may include a checksum that is later used to verify that the response is a correct response. Nowhere, however, does *Bryant* provide any teaching, suggestion, or incentive for comparing the set of identifiers used to reach the content with a return identifier to generate a response to indicate whether monitoring of access to the content is occurring.

Further, such a feature is not explicitly taught and is not inherent. Inherency is a concept that is used with respect to anticipation. The examiner is attempting to assert that this particular feature is inherent within *Bryant*. Such an assertion is incorrect based on

the section of *Bryant* cited by the examiner. This section above teaches that characterizations can be made with respect to the response received from the server. *Bryant*, however, provides no teaching, suggestion, or incentive as to how such a characterization is made. *Bryant* gives one possible example, but does not state that this is the necessary characterization that is made. *Bryant* indicates that this is only an example, which means other types of verifications may be made. Under the principles of inherency, a claim is anticipated if a structure in the prior art necessarily functions in accordance with the limitations of a process or method claim. In re King, 801 F.2d 1324, 231 U.S.P.Q. 136 (Fed. Cir. 1986). A prior art reference that discloses all of a patent's claim limitations anticipates that claim even though the reference does not expressly disclose the "inventive concept" or desirable property the patentee discovered. *Verdgaal Brothers, Inc. v. Union Oil Company of California*, 814 F.2d 628, 2 U.S.P.Q.2d 1051, (Fed. Cir. 1987). It suffices that the prior art process inherently possessed at that property. *Id.* Mere possibilities or even probabilities, however, are not enough to establish inherency. The missing claimed characteristics must be a "natural result" flowing from what is disclosed. *Continental Can Co. v. Monsant Co.*, 948 F.2d 1264, 20 U.S.P.Q.2d 1746 (Fed. Cir. 1991). Unstated elements in a reference are inherent when they exist as a "matter of scientific fact". *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 7 U.S.P.Q.2d 1057 (Fed. Cir.), *cert.denied*, 488 U.S. 892 (1988) and *Hughes Aircraft Co. v. United States*, 8 U.S.P.Q.2d 1580 (Ct. Cl. 1988). Otherwise, the invention is not inherently anticipated.

A feature is inherent only if such a feature must necessarily follow. Such a situation is not present in *Bryant*. In this case, *Bryant* teaches that characterization of a response may be used to verify the response. The comparison made is matching a checksum to fully parsing and analyzing the HTML response. It does not necessarily follow that a set of identifiers is compared to a return identifier. In claim 8, the set of identifiers includes a first number of identifiers sent by the requestor to the source to request the content and a second number of identifiers returned to the source in which the second number of identifiers represents a location of the content. The comparison of the return identifier from the response generated by the new request is not compared to the

set of identifiers in *Bryant*. Further, it does not necessarily follow that such a step occurs because *Bryant* teaches that a number of different types of comparisons may occur.

Therefore, it is not inherent that the comparing of a set of identifiers to a return identifier would occur because such a comparison does not necessarily follow from the disclosure in *Bryant*. Consequently, the comparing feature is not taught or suggested by *Bryant*. Further, no teaching, suggestion, or incentive is found in *Junkbusters* alone or in combination with *Bryant* for such a feature.

The other claims are independent claims containing features similar to independent claims 1 and 8. Thus, these claims are patentable over the cited references for the same reasons as independent claims 1 and 8. The other claims are dependent claims depending from one of the independent claims. These claims are patentable over the cited references for the same reasons. Further, these dependent claims include other features not taught or suggested by the cited references.

III. Conclusion

It is respectfully urged that the subject application is patentable over *Bryant* and *Junkbusters* and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 8/26/04

Respectfully submitted,

Duke W. Yee
Reg. No. 34,285
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorney for Applicant